Smart Card Procedures and Usage Policy **Document Control
A. Confidentiality Notice**This document and the information contained therein is the property of Shifa Medical Practice.
This document contains information that is privileged, confidential or otherwise protected from disclosure. It must not be used by, or its contents reproduced or otherwise copied or disclosed without the prior consent in writing from Shifa Medical Practice.
**B. Document Details**

|  |
| --- |
| **Classification:** |
| **Author and Role:**  | Dr Rashid |
| **Organisation:**  | Shifa Medical Practice |
| **Document Reference:** |  |
| **Current Version Number:** |  |
| **Current Document Approved By:** |  |
| **Date Approved:**  | 01/04/2019 |

**C. Document Revision and Approval History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Next Review  | Version By | Approved |  |
| 01/04/2019 | 01/04/2020 | Zahid Karim | Dr Rashid |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Shifa Medical Practice**

 **Smart Card Procedures Document**

**Background**

With the introduction of the NHS Care Records Service (NHS CRS) applications, it is of paramount importance that patients of the NHS are confident that their medical records are being appropriately kept secure and confidential in line with the NHS Care Records Guarantee.

To achieve this objective, all NHS Care Records Service compliant applications require healthcare professionals / workers requiring access, to be registered and issued with a Smartcard and have appropriate access profile(s).

The NHS CRS and related services like Choose and Book and the Electronic Prescription Service use a common approach to protect the security and confidentiality of every patient’s personal and health care details.

NHS CRS smartcards help control who accesses the NHS CRS and what level of access that they can have. They are similar to a chip and pin credit or debit card, but are more secure. A user’s smartcard is printed with their name, photograph and unique user identity number.

**Registering as a Smartcard User**

The Registration process comprises three distinct activities:
1) ***Registration of identity***:

A user is ‘sponsored’ to be issued with a Smartcard. The user has their identity checked to eGif level 3 and a personal details record is created in the Spine User Directory (SUD). This registration procedure will only need to be performed once, by a Registration Authority Agent or Manager.

2) ***Choosing appropriate access to NHS CRS functionality / information (via their profile) and linking it to the SUD record***:

This may be changed as necessary (by each organisation); a profile requires a sponsor’s approval which is granted by a Registration Authority Agent or Manager.

***3) Creating a card to link the user to their SUD record and access profile(s):***This allows access to NHS CRS. Doc. Ref – Version – Filename: Smart Card Procedures and Usage Policy Page 3 of 8

**New Staff Starting Work**As part of their normal induction process, new staff who are required to use the Practice Clinical System / NPfIT Application will be:
• Introduced to their relevant ‘sponsor’ who will identify their appropriate role profile and take them through the specific Registration Authority (RA) processes required. This could be how to become registered or, if the User already holds a Smartcard issued by another Practice, adding the necessary Role Profile/s.
• Trained on the aspects of the Practice Clinical System / NPfIT Application relevant to their role/s. (This guidance must be written as well as verbal).
• Trained on the National and Local CCG RA processes. Where full registration is required, the Applicant will be required to bring suitable forms of
identification with them. Where staff are recruited to a role which requires access to Clinical System / National NPfIT Applications it is important that the following points are considered:
• Checks on an applicant’s ID are made during recruitment to ensure that RA Level 3
identification requirements are met.
• Offers of employment are dependent on the applicant’s ability to meet and continue to meet all requirements for NPfIT access.
• The Induction process incorporates the issuing of Smartcards (where the applicant is not an existing Smartcard holder) and adding the appropriate role profile(s).
• Staff should be trained sufficiently prior to them using Smartcards and / or Clinical Systems / NPfIT Applications.

• Staff must have read and understood the policies and procedures governing the use of Smartcards, the Practice Clinical System / NPfIT Applications (as specified in RA01 form) and must sign to verify this. • All Clinical System / NPfIT Application Users must have sufficient training to carry out their Clinical System / NPfIT Application tasks without risk. To minimise duplication, all the above requirements will be integrated as much as possible into the Practice’s standard employment processes and procedures.

**Existing Staff Leaving the Practice**When existing staff members leave the Practice, the following points must be considered:
• All Practice role profiles in the NPfIT Spine User Directory pertaining to the employee will be deactivated as soon as is practical.
• If the User is transferring to another NHS related location (e.g. GP Practice, Acute Trust etc.) and they can provide details / proof, then the current registration details will be copied and sent to the new location – the user is allowed to retain the Smartcard but their Practice profile is removed.
• Staff permanently leaving the NHS (e.g. retirement, leaving for employment in a non-NHS job or taking up full-time education etc.) will have their certificate revoked and the Smartcard issued to them will be destroyed.
• The RA Manager must be advised, giving as much notice as possible.
• The required actions must be taken as soon as possible after the staff member leaves.

**Contractors**

The Practice will ensure all contractors who need to use the Clinical System / NPfIT Applications are bound to the Data Protection Act and The NHS Confidentiality Code of Practice.

This will include the process to be taken in cases of a breach and liability issues.

**Incident Reporting**

Incidents may be reported by any member of staff where they feel there is a risk to patient health, confidentiality or the reputation of the Practice.
Incidents should be reported, using the Practice Incident Procedure, to the RA Agent either within the practice or CCG and then escalated to the RA Manager of the CCG.
Examples of incidents to be reported include (list is not exhaustive):
• Smartcard or application misuse
• Smartcard theft
• Non-compliance of local or national RA policy
• Any unauthorised access of Clinical System / NPfIT Applications
• Any unauthorised alteration of patient data
The RA Manager will consider all incidents reported to them.
Any incidents considered significant will be escalated to the CCG Board / Senior Practice staff, HR and / or the Practice’s Caldicott Guardian depending on the nature of the incident.

A major breach of security will also be reported by the RA Manager to the LSP and NPfIT to ensure any risks resulting from the event can be taken into account and mitigated against.

A significant incident is an isolated incident or a series of less significant incidents that could lead to a serious degradation of healthcare or information security.
The Practice’s Caldicott Guardian will consider incidents reported to them and decide whether the Practice’s systems or working practices should be reviewed as a result.
Incidents which involve breaches of security or demonstrate that a User may not be considered trustworthy will also be reported to HR and the Practice’s Caldicott Guardian by the RA Manager so that any disciplinary measures required may be taken.
Dr. Rashid will decide which other members of staff need to be involved (e.g. Line
Manager, IT manager).

**Staff Responsibilities in the use of Smartcards**

Smartcards give users access to N3 connectivity and all of the services made available to general practice by Health and Social Care Information Centre (e.g. Choose and Book, Electronic Prescription Service, GP2GP, Summary Care Record)
All members of staff that require access to the Practice’s Clinical System must apply for and be issued with a Smartcard.

Smartcards are the property and responsibility of the user whilst they are employed at the Practice Smartcards must:
• Only used by the person named on the Smartcard;
• Never be shared;
• Be used every time the Practice’s Clinical System is accessed;
• Be removed from the Keyboard’s cardholder when the user finishes their work on the computer;
• Be kept safe at all times (cardholders on neck cords / clips have been issued to ensure safe keeping). Smartcards that develop technical problems (e.g. will not connect to the server) must be reported to the Manager immediately, so that appropriate action can be taken.
If a user leaves their Smartcard at home, they will be asked to return to collect it. Under no circumstances will the clinical system be accessed using another user’s card. Any violation of this rule will result in disciplinary action.

A member of staff going on long term sickness / maternity leave will be required to surrender their Smartcard to the Manager, so that the properties on the electronic chip can be removed.

These properties will be reinstated when the member of staff returns to work.

Staff leaving the Practice to move on to another NHS employer, and they can provide proof of this, will have the Practice properties removed from their Smartcard by the IT department. This will enable the Smartcard to be re-used by the new employer who will allocate their own properties to the Smartcard’s electronic chip.

**Effects of inappropriate use / misuse of Smartcards**

Inappropriate use of Smartcards may result in data being recorded on the Practice’s Clinical System but not being uploaded to the National spine. This could have serious consequences for third parties accessing data (with appropriate data sharing agreements in place) who will act on the information that is made available to them.
Smartcard misuse may also result in patient records not being complete, accurate, relevant, accessible and timely (e.g. for clinicians working in Out Of Hours).

**Ensuring Smartcards are used correctly**

The manager is the Practice person responsible for monitoring correct and appropriate use of Smartcards throughout the Practice and ensuring that they are used in accordance with the terms and conditions set out in the RA01 Short Form.
Copies of the RA01 Short Form are available from the manager.
Members of staff using Smartcards are required to sign a copy of the RA01 Short Form. The signed copy is stored in their Personal File.
To ensure that all members of staff issued with a Smartcard continue to be aware of the obligations set out in the RA01 Short Form, every person listed on the Smartcard Terms and Conditions Log Sheet (**See Specimen Template in Appendix A**) will verify s/he has read, understood and will comply with the obligations identified in the document by signing this Log Sheet in the appropriate place.

**Breaches of Smartcard Terms and Conditions of Use**

The Practice will ensure that all members of staff issued with a Smartcard are aware of the terms and conditions of issue and use, are able to comply with these and understand that failure to do so will be dealt with as a serious disciplinary matter.
Should there be any breach of the Smartcard terms and conditions of issue and use, the incident will be recorded in line with the Practice’s Incident Management Reporting Procedures and this in turn may lead to disciplinary action being taken against the individual(s) in question.

**Guidance Notes for the Practice on the issue and use of Smartcards
Introduction**

All organisations need to ensure that staff members and those working on behalf of the organisation who have been issued with an NHS Smartcard comply with the terms and conditions detailed in the RA01 Short Form.

Breach of the terms and conditions and/or of organisational procedures relating to Smartcard usage should be linked to incident management reports and disciplinary measures.
1. NHS Care Records Service (NHS CRS) Smartcards and pass codes help control who accesses the NHS CRS and what level of access that they can have.
Before a Smartcard is issued, the Registration Authority (RA) will require applicants to fill in and sign a RA01 form, thereby agreeing to the terms and conditions of issuance set out on the form.
2. From March 2010 the registration software will progressively change and new users will be required to sign these terms and conditions electronically, rather than in paper form, before being able to access any application.
Additionally any changes to the terms and conditions, or required resign of the terms and conditions, can be imposed by the software with further access being potentially denied if appropriate.

**Compliance with the Terms and Conditions of Smartcard Issue**

1. These conditions are in part no more than the information governance practice required of all staff but there are also a number of key requirements around the safe and secure retention of Smartcards and the notification of any changes to the user’s access profiles.
2. It is essential that everyone with an NHS Smartcard and pass code is aware of and able to comply with the terms and conditions of issue and that they understand that failure to do so will be dealt with as a serious disciplinary matter.
3. If the Smartcards and pass codes have been issued via another organisation’s RA (e.g. by a CCG to a general practice), then the provider organisation will require assurances.
These assurances will include evidence of periodic review that practice partners, owners,
senior managers, etc. are aware of and complying with their responsibilities to:
• Monitor staff compliance with the terms and conditions of smartcard usage;
• Inform the provider organisation when staff leave or change jobs;
• Report any usage issues.
4. All organisations, whether they are a Registration Authority or not, that have NHS Smartcard users must have effective and clearly defined procedures for dealing with breaches in the use of Smartcards and pass codes.
These procedures need to be organisation-based so that appropriate action can be taken by the user’s employer and should integrate with existing Human Resources and information security procedures.
5. Organisations with Registration Authority responsibilities should ensure these procedures are incorporated into their overall RA business processes and procedures.
6. All Smartcard users must be effectively informed about the procedures for dealing with a breach.
**Appendix A - Smartcard Terms and Conditions Log Sheet
I have read and understand my responsibilities with regard to the terms and conditions set out in the RA01 Short Form**

**Appendix A - Smartcard Terms and Conditions Log Sheet**

**I have read and understand my responsibilities with regard to the terms and conditions set out in the RA01 Short Form**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Date RA01Short FormReviewed | **Name** | **Position/ Work Role** | **Date Smartcard Issue** | **Smart Card Expiry Date** | **Signature** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |